proofpoint.

GUÍA DE COMPRA

Guía para CISO sobre cómo bloquear las amenazas centradas en las personas y la IA

Características principales

Estas son las cinco funciones que necesita para proteger su organización frente a las amenazas centradas en las personas y en la IA:

1. Visibilidad completa de las amenazas y análisis de riesgos
2. Protección automatizada contra amenazas por correo electrónico y otros vectores
3. Seguridad para comunicaciones empresariales de confianza
4. Orientación para los empleados
5. Protección frente a la usurpación de cuentas

Descripción general

Los ciberdelincuentes no escatiman esfuerzos a la hora de filtrar datos y explotar las comunicaciones empresariales con fines lucrativos. Pero mientras el volumen de amenazas sigue creciendo, las tácticas empleadas permanecen prácticamente inalteradas. El phishing, el malware, el ransomware, los ataques Business Email Compromise (BEC) e ingeniería social siguen siendo los métodos preferidos para atacar a los usuarios.

Lo que sí ha cambiado, sin embargo, es que la IA optimiza estas tácticas ya conocidas. Los ciberdelincuentes utilizan grandes modelos de lenguaje a gran escala para crear mensajes de phishing hiperpersonalizados, automatizar entre el 80 % y el 90 % de la cadena de ataque y lanzar campañas multicanal en varias fases a una escala sin precedentes. En 2025, Proofpoint observó un aumento del 94 % en las amenazas por correo electrónico dirigidas a los clientes. La IA también introduce nuevas vías de ataque, como los ataques por inyección de prompts. Estos aprovechan los asistentes de IA corporativos insertando instrucciones ocultas en los correos electrónicos.

En esta guía, analizaremos las principales funciones que necesita su empresa para establecer un sistema de defensa eficaz contra todas las amenazas centradas en las personas y la IA, ya sea que se transmitan por correo electrónico o a través de otros vectores. También le sugeriremos varios criterios que le servirán de guía a la hora de elegir una plataforma de seguridad que se adapte a sus necesidades.

Figura 1: Amenazas y riesgos en los entornos de trabajo digitales

1: Visibilidad completa de las amenazas y análisis de riesgos

Para bloquear las amenazas centradas en las personas y la IA, es necesario determinar quiénes son los usuarios objetivo y cómo se dirigen a ellos. Esto le permite aplicar controles de seguridad adaptativos para proteger a las personas que corren mayor riesgo.

Una visibilidad completa de las amenazas que abarca el correo electrónico y los canales digitales le ofrece una visión global de sus vulnerabilidades.

Estos son los elementos sobre los que una solución debe darle esta visibilidad:

- **Personas a las que se dirigen, amenazas a las que se enfrentan y cualquier interacción que hayan tenido con los ciberdelincuentes.**
- **Información forense**, como el ciberdelincuente implicado, la familia de amenazas, los usuarios afectados, las técnicas de ataque, los temas explotados y los objetivos de la campaña de ataque.
- **Usuarios de riesgo**, identificando quién representa un riesgo para su organización y por qué.
- **Amenazas asociadas a las comunicaciones corporativas de confianza**, incluidos dominios o sitios web falsos y parecidos que pueden dañar la imagen de su marca.
- **Cambios en el comportamiento e inteligencia de amenazas**, que pueden revelar que uno de sus proveedores o un tercero de confianza puede haber sido comprometido.
- **Actividades sospechosas**, que podrían indicar posibles usurpaciones de cuentas

Una plataforma optimizada mediante IA puede correlacionar las señales en todas estas dimensiones, utilizando grafos de relaciones para establecer una referencia de los comportamientos comunicativos normales, modelos lingüísticos para interpretar la intención del mensaje e inteligencia de amenazas para contextualizar el comportamiento de los ciberdelincuentes. De este modo, obtendrá información sobre los riesgos más precisa y útil que la que proporciona un simple análisis manual.

La visibilidad no solo es importante durante los despliegues iniciales, también debe ser constante. Esto significa que puede ajustar su nivel de protección continuamente, tan pronto como cambien las características de los ataques.

4,88 M$

Coste medio de una fuga de datos causada por un ataque de phishing o BEC[1]

1. Informe *sobre el coste de una fuga de datos de IBM*, 2024.

2: Protección automatizada contra amenazas para el correo electrónico y otros vectores

El panorama de amenazas evoluciona constantemente. Por desgracia, las organizaciones a menudo carecen del talento en seguridad y de los recursos necesarios para mantenerse al día. En consecuencia, los equipos no suelen tener tiempo para investigar todos los incidentes de seguridad. Además, el coste de los incidentes va en aumento.

Por eso necesita una solución que pueda detectar y bloquear las amenazas con precisión y eficacia, sin afectar a la productividad. A medida que la IA desempeña un papel cada vez más importante en la generación y notificación de amenazas, resulta imprescindible optimizar también las funciones de detección mediante IA

Estas son todas las acciones que una solución debería poder realizar automáticamente:

- **Bloquear las amenazas antes de la entrega** con una eficacia mínima del 99,999 % para que nunca lleguen a las bandejas de entrada de sus usuarios.
- **Detectar y bloquear amenazas generadas por la IA**, incluidos los mensajes BEC generados por IA, el phishing personalizado mediante IA y los ataques de inyección de prompts ocultos dirigidos a asistentes de IA como Microsoft Copilot.
- **Analizar los patrones de comportamiento de los correos electrónicos enviados internamente**, utilizando inteligencia de amenazas optimizada mediante IA y modelos de aprendizaje automático para detectar actividades de phishing lateral.
- **Examinar y bloquear URL maliciosas en tiempo real** para garantizar que no lleguen a los usuarios a través del correo electrónico o las plataformas de mensajería y colaboración.
- **Detectar y neutralizar cuentas comprometidas de proveedores de identidad** alojadas en la nube.
- **Analizar los códigos QR sospechosos antes de su entrega** mediante visión artificial optimizada con IA, análisis semántico y en entorno aislado (sanbox).
- **Insertar etiquetas de advertencia** en los mensajes sospechosos.

Cuando un ataque consigue el acceso inicial, es vital poder detectar y neutralizar la amenaza rápidamente. Esta rápida actuación puede marcar la diferencia entre un incidente menor y un compromiso a gran escala.

3: Seguridad para comunicaciones empresariales de confianza

Las comunicaciones digitales son vitales para las organizaciones. Por eso no es de extrañar que los ciberdelincuentes hagan todo lo posible por infiltrarse en las comunicaciones de confianza. Ataques como el phishing, el ransomware o Business Email Compromise (BEC) tienen un mayor porcentaje de éxito cuando los destinatarios creen (erróneamente) que están interactuando con fuentes de confianza.

Para aumentar sus posibilidades de éxito, los ciberdelincuentes utilizan una amplia gama de tácticas de suplantación de la identidad. Estas se han vuelto mucho más eficaces gracias a la IA. Los ciberdelincuentes ahora pueden generar en cuestión de segundos mensajes bien redactados y adaptados al contexto, capaces de imitar el tono y el estilo de redacción de un directivo. Por lo tanto, es esencial establecer varias capas de protección para frustrar sus intentos.

- **Permita la autenticación del correo electrónico** generado por usuarios y aplicaciones.
- **Proporcione un entorno seguro y dedicado** para retransmitir los correos electrónicos transaccionales generados por las aplicaciones.
- **Ofrezca asistencia en la implementación de DMARC** para maximizar la eficacia de la autenticación del correo electrónico y garantizar la plena conformidad con DMARC.
- **Proteja contra "lookalike domains" (dominios parecidos)**, incluidas funciones de detección y asistencia para bloquear y desmantelar estos dominios maliciosos.
- **Supervise las cuentas de proveedores comprometidas** mediante la IA basada en el comportamiento y la inteligencia de amenazas, y la ejecución de acciones automatizadas para protegerse de ellas.

Al proteger sus comunicaciones empresariales de confianza, puede proteger no solo a sus empleados, sino también a sus partners comerciales y clientes.

4: Orientación para los empleados

Aunque la tecnología bloquee el 99 % de las amenazas, el 1 % restante puede dar lugar a un incidente grave. Aquí es donde el comportamiento humano se convierte en un factor crucial. Por lo general, los ciberdelincuentes necesitan que sus usuarios interactúen con ellos para llevar a cabo sus campañas maliciosas.

Y los ataques no son la única preocupación en este ámbito. A menudo, los usuarios sacrifican la seguridad de sus organizaciones en aras de la comodidad. Según el informe *State of the Phish* de Proofpoint:

- El 71 % de los empleados admite comportamientos de riesgo, como reutilizar contraseñas o hacer clic en enlaces desconocidos.
- El 96 % de estos empleados eran conscientes de que su comportamiento entrañaba riesgos, pero aun así llevaron a cabo las acciones peligrosas.

Con la creciente integración de las herramientas de IA en los flujos de trabajo diarios, los empleados también se enfrentan a nuevos riesgos, como el uso compartido de datos sensibles con aplicaciones de IA no autorizadas o la activación involuntaria de la inyección de prompts ocultos al interactuar con asistentes de IA.

Cuando se combinan los ataques con el comportamiento negligente de los usuarios, se multiplican las posibilidades de éxito. Por tanto, es esencial concienciar a los usuarios sobre la seguridad.

Busque una solución que:

- **Use datos sobre amenazas** para identificar a los usuarios más expuestos a riesgos.
- **Proporcione a los usuarios formación basada en riesgos** que utilice ejemplos de amenazas reales como los que realmente atacan a su organización.
- **Haga hincapié en impulsar un cambio de comportamiento**, en lugar de formar a los usuarios simplemente para que marquen una casilla en la lista anual de tareas pendientes.
- **Motive a los empleados** dándoles visibilidad de su puntuación de riesgo individual, así como de su impacto en el nivel de seguridad de la organización.
- **Evalúe la eficacia** y elabore informes útiles para ayudarle a perfeccionar la estrategia.
- **Aborde los riesgos relacionados con la IA en los materiales de formación**, explicando, entre otras cosas, cómo utilizar las herramientas de IA generativa de forma segura e identificar los ataques de ingeniería social generados por la IA.

La tecnología de alto rendimiento combinada con la vigilancia humana es fundamental para bloquear las amenazas centradas en las personas. Todos y cada uno de nosotros desempeñamos un papel fundamental en la seguridad de las operaciones de la empresa.

71 %

de los empleados admiten comportamientos de riesgo, como reutilizar contraseñas o hacer clic en enlaces desconocidos[2].

2. Proofpoint. *Informe State of the Phish*, 2024.

5: Protección frente a la usurpación de cuentas

Los datos de Proofpoint muestran que el 99 % de las organizaciones experimentan regularmente intentos de usurpación de sus cuentas. Estos ataques son una forma de robo de identidad en la que un ciberdelincuente accede a una cuenta online y se hace efectivamente con el control de esta. Como era de esperar, los proveedores de identidad en la nube como Microsoft Entra ID, Google y Okta son los más atacados. Estas cuentas se utilizan para el inicio de sesión único (SSO) en una serie de aplicaciones empresariales.

Además, sus cuentas no son lo único de lo que debe preocuparse. Los ciberdelincuentes también comprometen las cuentas de partners comerciales de confianza para llevar a cabo operaciones de reconocimiento y lanzar nuevos ataques. Estas cuentas comprometidas sirven como puntos de entrada para lanzar ataques en varias fases que se propagan por todo el ecosistema de una empresa con el fin de robar datos sensibles, realizar transacciones fraudulentas y sembrar el caos.

La IA y el aprendizaje automático son fundamentales para supervisar las comunicaciones profesionales a gran escala y automatizar las respuestas. Los modelos de IA basada en el comportamiento pueden detectar las señales más sutiles de compromiso de una cuenta, como comportamientos inusuales en el inicio de sesión y el envío de correos electrónicos, o cambios en las relaciones de comunicación, que podrían pasar desapercibidos para los sistemas basados en reglas.

Busque una solución que:

- **Supervisa continuamente todas las cuentas** asociadas a servicios de proveedores de identidad en la nube, como Microsoft Entra ID, Google y Okta.
- **Usa Inteligencia de amenazas** combinada con datos de comportamiento y aprendizaje automático para detectar cuentas comprometidas.
- **Protege frente a los ataques de usurpación de cuentas** que eluden la autenticación multifactor (MFA); el 65 % de las cuentas pirateadas estaban protegidas por MFA[4].
- **Acelera las investigacionesgracias** a una visión centralizada de las actividades posteriores a la usurpación.
- **Automatiza la respuesta con acciones como la suspensión de cuentas, el** restablecimiento forzoso de contraseñas y la reversión de cambios maliciosos en las reglas del buzón y la configuración MFA.
- **Elimina aplicaciones sospechosas de terceros** como parte de la limpieza posterior de cuentas posterior a la usurpación.

La usurpación de las cuentas puede costarle caro a su empresa y dañar su imagen de marca. Una protección rigurosa es esencial para limitar el riesgo.

Evite enfoques fragmentados

Al establecer sus defensas para el correo electrónico y otros canales, las soluciones individuales de varios proveedores especializados pueden parecer la opción lógica. De hecho, estos proveedores parecen perfectamente preparados para responder a determinados tipos de ataque. Sin embargo, este enfoque aislado presenta una serie de inconvenientes.

En primer lugar, crea ángulos muertos de seguridad. Cuando las herramientas no están totalmente integradas, los equipos de seguridad tienen dificultades para obtener visibilidad de todo el entorno de seguridad. Esta visión parcial aumenta el riesgo de que las amenazas escapen a la detección, además de retrasar la respuesta a los incidentes.

Las herramientas fragmentadas tampoco pueden ofrecer el enfoque integral de la IA necesario para bloquear las amenazas actuales. Los modelos de lenguaje, la visión artificial, el análisis de comportamiento y la inteligencia de amenazas deben funcionar necesariamente de forma coordinada y compartir datos contextuales para detectar los ataques sofisticados generados por la IA.

Además, la gestión de varias herramientas de seguridad supone una tarea que requiere mucho tiempo y resulta poco eficaz para los equipos, que además deben correlacionar los datos procedentes de puntos de control aislados entre sí. Por no hablar de que el considerable volumen de alertas que generan estas plataformas acaba provocando una disminución de la atención prestada a dichas alertas y un mayor riesgo de pasar por alto ciertas amenazas. Todos estos factores aumentan los costes operativos.

Así que opte por un enfoque más eficaz. Adopte una plataforma de seguridad completa y preintegrada que le proteja contra todas las amenazas centradas en las personas. Además, trabajar con un único partner de confianza no solo garantiza una gestión ágil, sino que también reduce los costes.

99 %

de las organizaciones sufren regularmente intentos de usurpación de cuentas[3].

3. Investigación de Proofpoint
4. Ibid.

Conclusión

Una estrategia de seguridad integral centrada en las personas le ayuda a proteger su organización frente a una amplia gama de amenazas. Para alcanzar este objetivo , hay que empezar por elegir la solución adecuada. Opte por una solución que reúna inteligencia de amenazas procedente de distintos vectores: correo electrónico, herramientas de colaboración, plataformas de mensajería y aplicaciones cloud. También debe proporcionar información relevante sobre los comportamientos de riesgo de los usuarios y contribuir a reforzar su cultura de seguridad.

¿Su solución actual se limita al correo electrónico? ¿O utiliza soluciones individuales y fragmentadas? Si es así, seguro que puede mejorar. Ha llegado el momento de evaluar la eficacia de sus dispositivos de seguridad actuales frente a todas las amenazas centradas en las personas, para el correo electrónico y para muchos otros vectores.

Consolide sus defensas con Proofpoint

Proofpoint Prime Threat Protection ofrece una plataforma de protección contra amenazas preintegrada para una seguridad completa. Proofpoint Prime bloquea las amenazas en los entornos de trabajo modernos, incluidos el correo electrónico y los canales digitales. La plataforma no solo le protege frente a una amplia gama de amenazas, sino que lo hace con una precisión de detección inigualable. Optimizada por la plataforma Proofpoint Nexus AI, un conjunto de motores de IA que incluye modelos de lenguaje, aprendizaje automático, visión artificial, grafos de relaciones e inteligencia de amenazas, Proofpoint Prime ofrece una eficacia de detección del 99,999 % frente a amenazas tradicionales y generadas por IA.

También proporciona información detallada sobre el factor humano de riesgo y refuerza la resiliencia de los usuarios. Por último, le protege contra cuentas de usuarios y proveedores comprometidas, para que sus comunicaciones empresariales sigan siendo seguras.

Proofpoint ofrece la única arquitectura de ciberseguridad moderna con un enfoque adaptable para proteger los recursos más importantes y de mayor riesgo de su empresa: sus empleados. Por eso, más de 2,7 millones de clientes de todos los tamaños, incluidas más de 80 de las empresas Fortune 100, confían en Proofpoint.

proofpoint.

DESCUBRA LA PLATAFORMA DE PROOFPOINT →